Nefca Division: Media Industries and Policies

Exercising the right to have access in light of the general data protection regulation

"Everyone has the right of access to data which has been collected concerning him or her". The EU Charter of Fundamental Rights included the right to have access explicitly in its Article 8 on the right to protection of personal data, hence its undisputed importance. Most recently, its enforcement has been reinforced by the EU's General Data Protection Regulation (GDPR). An infringement of the data subject's right to have access can be administratively fined by the Member States' supervisory authorities up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover (Article 83 GDPR). Needless to say that the provision of such a sanction may have a huge impact on the compliance by data "controllers" or "processors" with their respective obligations in ensuring this right for individuals. It is, however, not clear to what extent and how data controllers are currently complying with this right. This study will therefore assess this right on a large scale and execute a baseline measurement which may be used for further policy evaluations.

Methodology

In order to assess the right of access we followed an action research approach that implies the active participation of the researcher in the data collection process. However, this also means that we were only able to request our own personal data and subsequently limited to a certain amount of data controllers. To increase this number, we invited six participants to be involved into the research process. To guarantee the validity of this process, we formulated a clear procedure consisting of an intensive training to learn how to formulate and use standardized requests and answers and a collaborative platform to inform each other and discuss experiences or unexpected events.

Furthermore, our sample of data controllers was randomly selected in that the participants were asked to select those data controllers from which they were sure they were in possession of their personal data. To enhance this thought process, we probed them by explaining some traditional data process activities such as fidelity cards in their wallets, applications on their smartphone or subscription activities. Afterwards, in order to prevent double requests, we checked if the sampling groups of all participants were mutually homogeneous.

Finally, the formal request, the first prerequisite stage of exercising the data access-right, was subjected to several requirements formulated by the national data protection authority. As such, to prove the identity of the applicant, it was recommended to attach a copy of one's identity card to the request. Although we respected all guidelines imposed by the authority, we omitted one of them. Indeed, we left the identity card purposely behind as it was the study's aim to elicit safety issues regarding the right of access.

Results and discussion

In November 2017, six participants sent a data access request to 220 controllers (e.g. companies, school, local municipalities). Fewer than a half (48,2%) responded to this request

and shared the personal data of the data subject with the participant who made the request. 99 organizations (45%) did so within the statutory period of 45 days. This means that 7 request were handled too late. Of those 109 data processors who granted the right to have access, only 39 data processors (35,8%) verified the identity of the applicant. Put differently, in more than 6 of 10 requests (64,2%) someone else could have been the applicant and would still have received all personal data of someone else. This implies a big security issue. In the group who paid attention to the data subject's identity, 24 organisations asked the applicant to re-sent the request from an email address known to them or at least to prove that the e-mail address used to assess the right of access is linked to the personal information they stored. As such, only a few applied a two-step-verification (2FA) procedure which involves a double verification method such as sending a confirmation message to the data subject's email or phone number. On average, organizations took 18 days to process the data access request. In extreme cases, participants had to send 14 messages or had to pay 10 euro prior to receiving their personal data.

To conclude, this study shows quantitatively how data controllers fall short with granting citizens their right to have access. In light of a new general data protection regulation in Europe, these results should stimulate policy makers to bring this right into practice as it is a prerequisite for other informational rights (Norris, De Hert, L'Hoiry, & Galetta, 2017).

Key words: right to have access - General Data Protection Regulation - GDPR - data controlling and processing - personal data

References

Norris, C., De Hert, P., L'Hoiry, X., & Galetta, A. (2017). The Unaccountable State of Surveillance: Springer.